

## Extreme IR Reader

Software for  
Reading data via IR

Page 2

## Extreme MB Tool

Software for Hash  
and Key  
Calculations

Page 3

## Extreme EZS reader

Software for  
Reading data via  
IR from the EZS

Page 4

# Extreme MB TOOLS

*The best MB solutions*

## Extreme BE Key programmer

Software for BE  
key programming  
via IR

Page 5



## Extreme EZS Password reader

Software for  
Reading Password  
direct from EZS  
via IR

Page 6

## Extreme All Keys Lost

Software for  
reading data from  
EZS in All Keys  
Lost situation

Page 7

Complete key  
programming  
procedure when a  
working Key is  
available

Page 9

# Extreme IR Reader

## 1. Key ID

Displays Keys SSID

## 2. Status

Displays Status of the Key

## 3. FW

Displays the Firmware version of the Key

## 4. Distance

Displays Hex value corresponding to the Keys Life Counter

## 5. Life

Displays the Keys Life counter. Actual number Of remaining times key will be operational

## 6. Get Data Button

Read the data from a working key that is then used to calculate the Key/EZS Password

## 7. EZS Hash

Current Hash Stored inside EZS for the Key that we are currently working with

## 8. Count

Remaining data to collect during Data Acquisition.

## 9. Check Password Button

Check if the Password is a match with the Key inserted in IR Programmer

## 10. Select

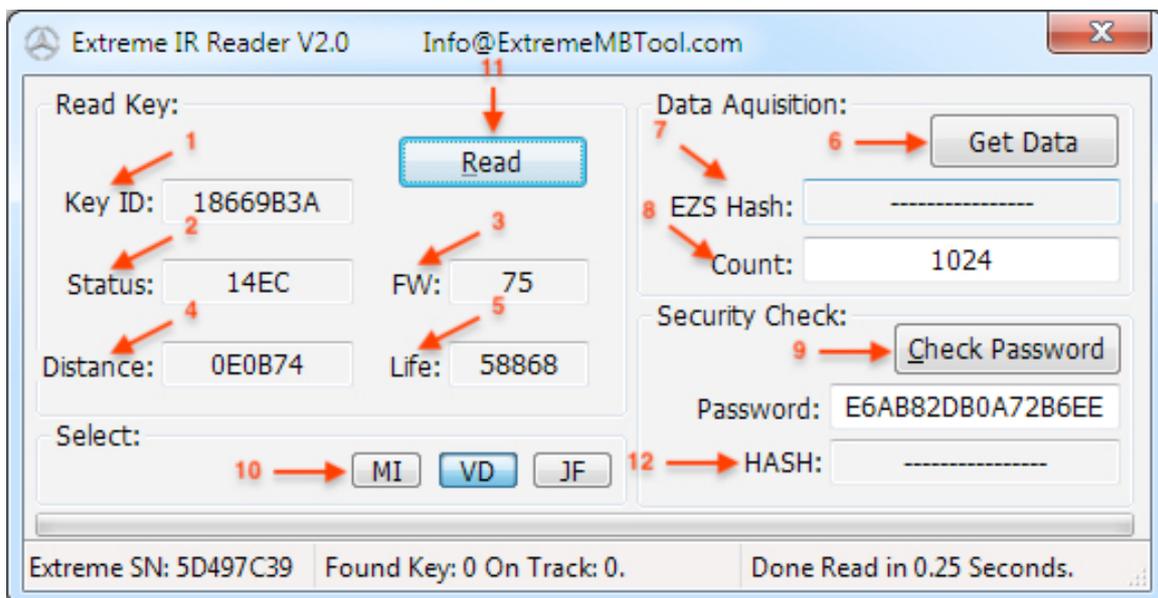
MI- VD- JF  
A choice of 3 different Random we use for Data acquisition.  
(Development only)

## 11. Read Data Button

Read info from Key such as SSID, Status, Life and Firmware

## 12. HASH

When the correct Password is entered in the Password field, then the "HASH" field will display the actual real decoded Hash being sent from the Key



# Extreme MB Tool

## A. Sonder Hash Calculation

A software option for calculating the "Dealer Password" for FBS3 components - EZS, ESL, 7G, ISM, ECU ...

## C. ESL Password Calculation

A software option used for the calculation of the Crypto ESL Password from KEY/EZS Password. Suitable for models W204/207/212

## B. SKC

A software option used to calculate the files to be written to the Keys from the data we read from the EZS.

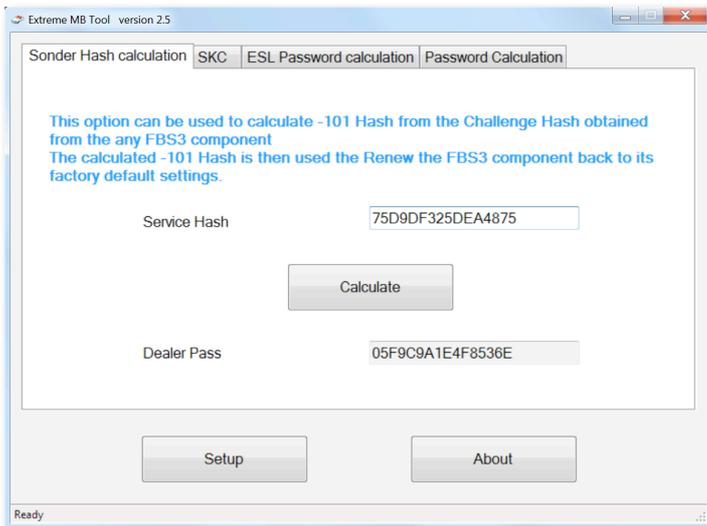
## D. Password Calculation

A Software option used to calculate the FBS3 password from a list of data collected from either the EZS or the Key.

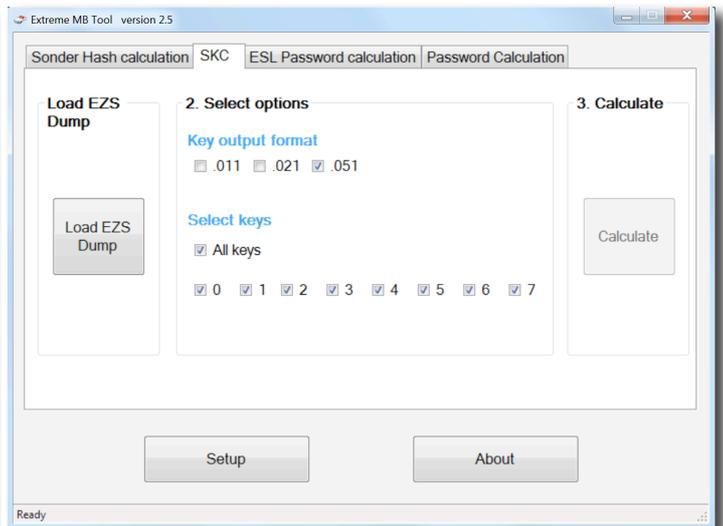
Customers with a valid annual subscription can use the software to calculate passwords for FREE. There are no TOKENS. There are limits for using each of the functions, but these limits are more than enough even for professional workshops:

- 3 FREE daily calculations for Sonderhash calculations (Dealer Hash)
- 3 FREE daily calculations for ESL Password Calculation
- 3 FREE daily calculations for calculation of key files from EZS dump
- 3 FREE daily calculations for EZS Password Calculation

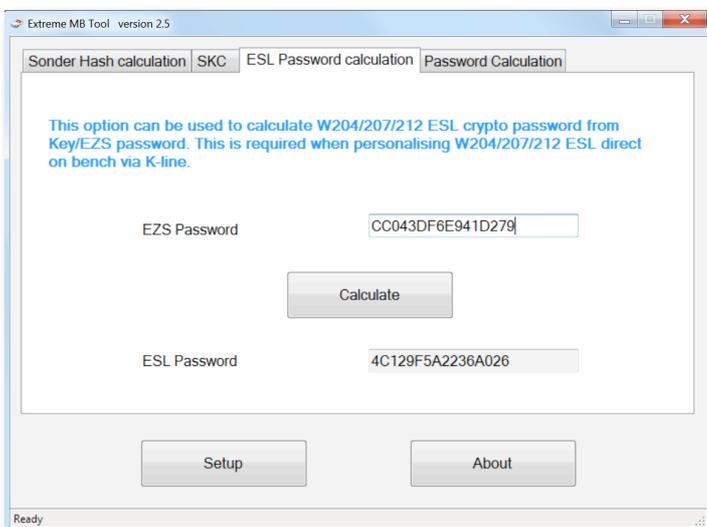
A



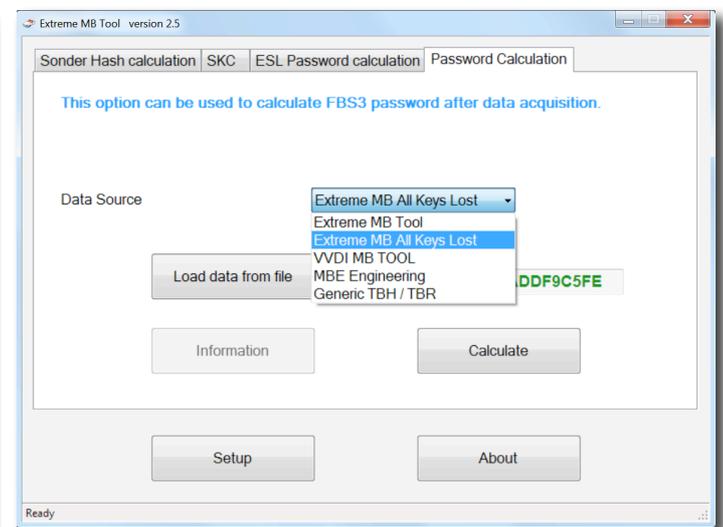
B



C



D



# Extreme EZS Reader

## 1. Hash

From H0 to H7 are the actual current key hashes for each Keys position

## 2. Used or Block positions

"Used" is occupied key position and "Block" is a blocked key position, also known as "Disabled Key"

## 3. Security

This field displays the SSID, Sonder and Serial number of the EZS. Also it has a field to paste the "Password"

## 4. Type II

For some different EZS types in order to read the data we have to select this option – this option is only needed for later NEC type EZS such as W166, W176, W246, W117

## 5. Ezs Read Button

We use this Button to "Read EZS" Before you press this button you should enter (or paste) the EZS Password into the "Password" field, When working on some EZS you will be prompted by the software to Re-insert IR KeyTool to EZS to complete the collection of data. Please follow the on screen instructions from Software

## 6. EZS Status

**Initialized** – EZS are initialized in factory

**Personalized** – EZS has been Personalized, meaning that FBS Data has been written inside (Hashes, SSID, Password...)

**Neutralized** – EZS has been Renewed sometime in the past using some tool. Usually this is the case when an EZS has been taken from another vehicle, Renewed, then re-adapted to match the current vehicle.

**TP Removed** – This is Transport Protection. TP must be removed before personalization process begins

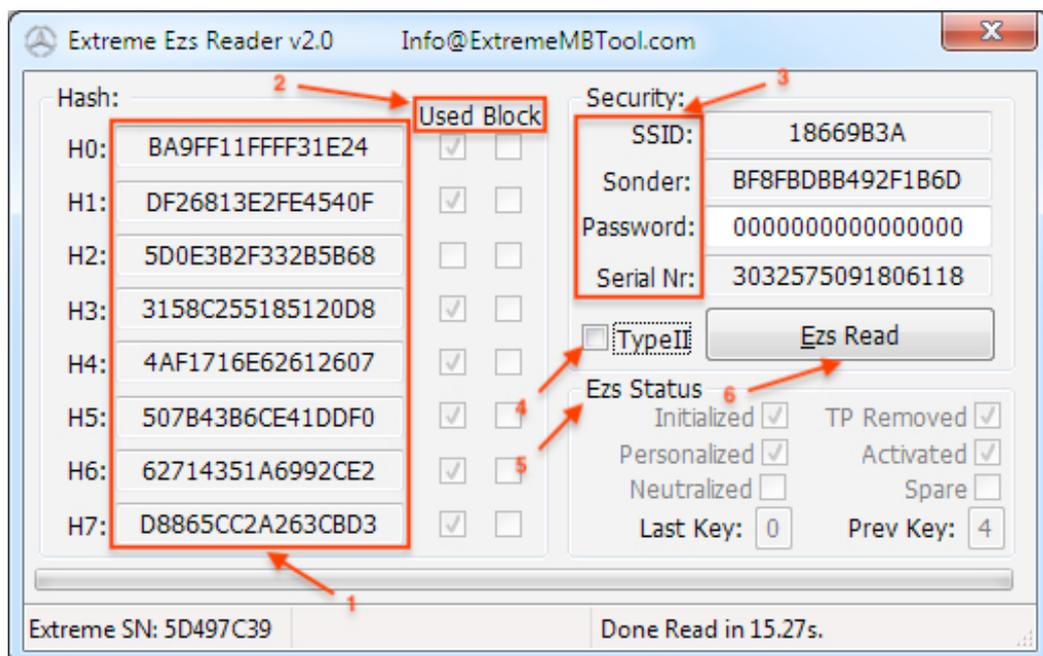
**Activated** – This means EZS is Activated. When an EZS is "Activated" it can no longer be personalized

**Spare** – This tells us that the EZS is a "Spare Part" EZS

"NOTE" There are 2 different types of EZS. 1.Series and 2.Spare. Series EZS are the original EZS that are installed during time of production inside Factory. Spare EZS are Replacement/Aftersales EZS

**Last Key** – The number indicates the last Keys Position Used

**Prev Key** – The number indicates the previous Keys Position Used



# Extreme BE Key Programmer

## 1. Read Key:

By pressing the "Read" button we can read various information from the BE Key, such as the Key ID, Status, Firmware, Distance and remaining Life of the key.

## 3. Select

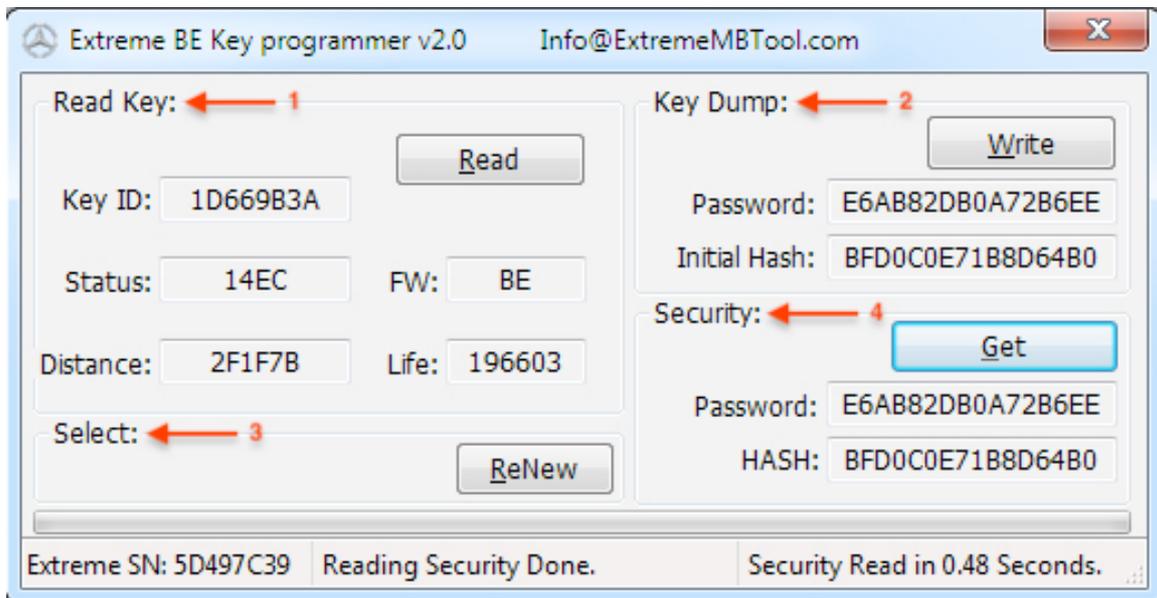
By pressing the button "ReNew" we can erase all the data inside the BE Keys Eeprom and give it status "21DF". This 21DF status means that the key is now ready to be programmed via IR with Programmer.

## 2. Key Dump

This is where you will load the Key file to be written to the BE Key. We simply press the button "Write" and the software will ask you to select a file, at this point choose the Key file that you wish to use, click open and the software will write the Key file directly into the BE keys Eeprom via IR

## 4. Security

By pressing the button "Get" you can read the BE Keys Password and current HASH direct from the BE Key via IR.



# Extreme EZS Password reader

## 1. SSID

This field Displays the SSID of the EZS

## 3. Password

**Password:** = This is the actual "True" EZS Password calculated and checked by our software, because we check the Password before it is displayed inside this field you can be 100% sure that it is a match with the EZS.

## 4. Enc. Pass

**Enc.Pass:** = Encrypted Password. When we see this Enc. Pass, this means that Password reading via IR is not supported on this EZS. The EZS has returned an encrypted response, we can only use this encrypted response to verify the true password if it is known.

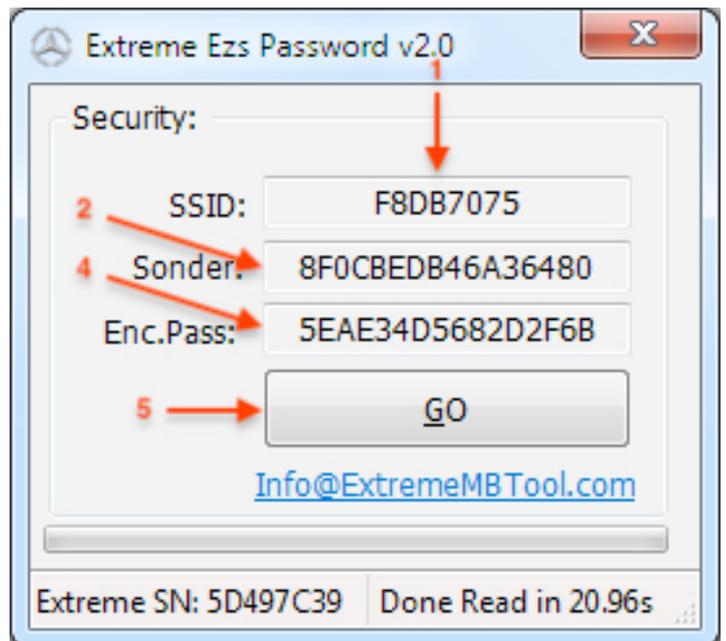
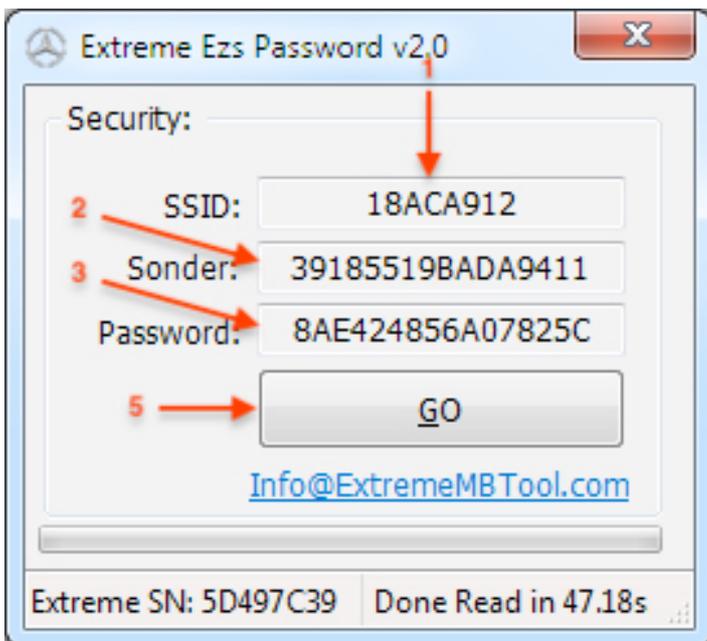
## 2. Sonder

This field displays the EZS Sonder Hash. Sonder Hash can be called different names depending on the tool manufacturer. It is good to understand that Sonder/Special and Service Hash are all same, only different terminology. Same goes for Dealer Password and Erase Password. From the Sonder you can calculate the Dealer Password needed to Renew EZS. You can calculate the "Dealer Password" using the Extreme MB tool software.

## 5. Go Button

Pressing the "GO" button will start the process of reading the EZS Password Via the IR Portal. This can take up to 3 minutes to complete. HC12 types are usually finished within 50 seconds, whereas HC908 types can take up to 3 minutes.

Read Password direct from EZS via IR. Support Old Motorola EZS with MCU's HC908 and HC12 inside EG: Some W203, W463, W209, W211, W215. Not support HC05, ST12 or ZGW types. Here is a list of tested Part Numbers: 2035450108, 2035450308, 2035450508, 2035450608, 2095450508, 2115450608, 2115451008, 2155450208, 2155450408



# Extreme All Keys Lost

## 1. AKL

When you select this option, it means that you will work with the "All Keys Lost" function within the software.

## 3. Counter

Remaining data to collect during Data Acquisition.

## 5. All Keys Lost Button

When you select the Checkbox "AKL" the text on this button is changed to "All Keys Lost" We click on it to begin the AKL procedure

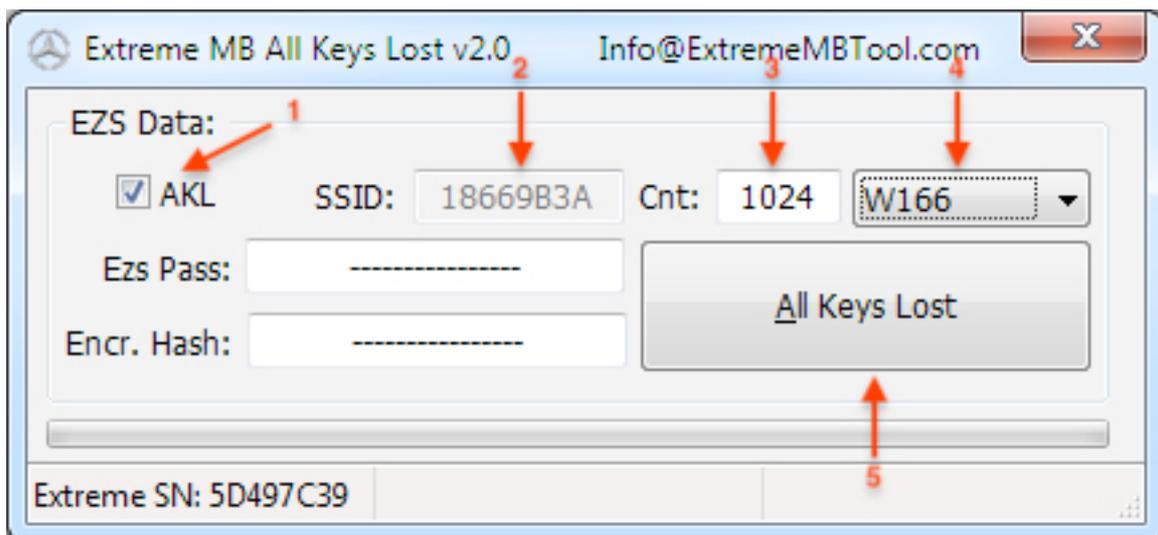
## 2. SSID

This field displays the SSID of the EZS

## 4. Drop down Menu

Here we select the Car model for All Keys Lost procedure. Supported currently are the following models with FBS3 -> W176 -> A-Class (2012-2014) W246 -> B-Class (2012-2014) W166 - M/GLE-Class (2012-2014) W117 -> CLA-Class (2013-2014) W212 -> E-Class (2009-2013); W218 -> CLS - Class (2011-2014) C197 ->SLS-Class (2010-2014)

**Further clarification:** This AKL procedure involves reading data direct from the EZS via the IR Portal. We collect 1024 individual data from the EZS within 6 minutes (older W212 EZS require 14 minutes) During the collection of this Data you will see the counter decrement from 1024 -> 0. When the data has been collected you will be asked to save a .akl file. This file can then be loaded to our server using the Extreme MB Tool Software and selecting "Password Calculation / Extreme MB All Keys Lost" This process would be the preferred method when working with Newer cars such as the W166, 246 and 176 because the time required to create a file is only 6 minutes and it does not effect the Key / EZS life at all. Also, using this method there are no risks of loosing sync with other control units / ESL as this sometimes can happen on these models when reading too many hashes from a working BGA key. This option to read data direct from the EZS via IR is a much safer option on these models.



# Extreme All Keys Lost

## 6. Ezs Pass:

We can use this field to enter a Password to check if it is in fact a match with EZS. This Password can be calculated using the Extreme MB tool software.

## 8. Erase Hash

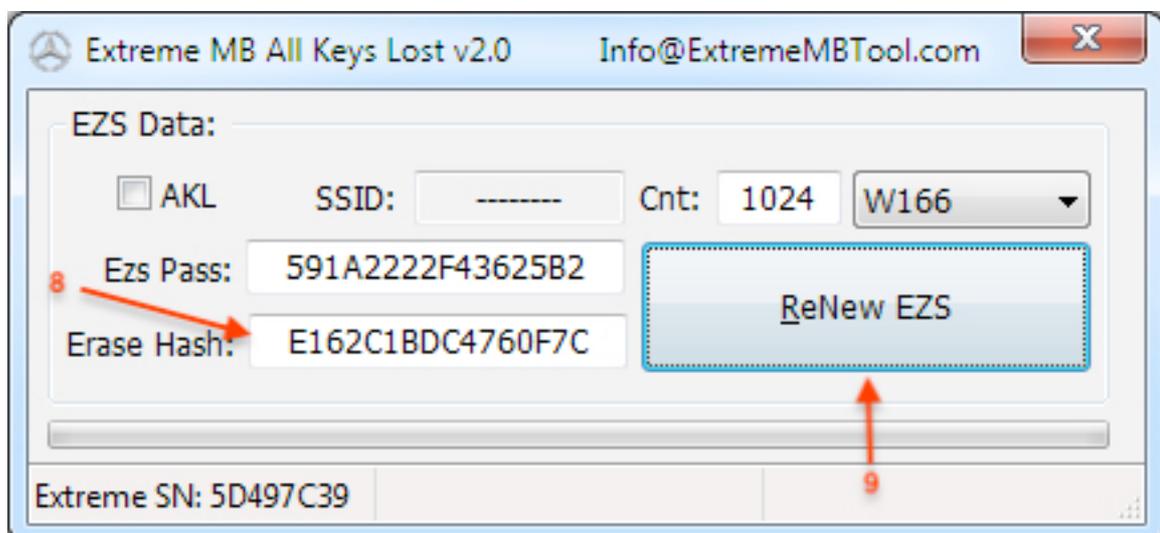
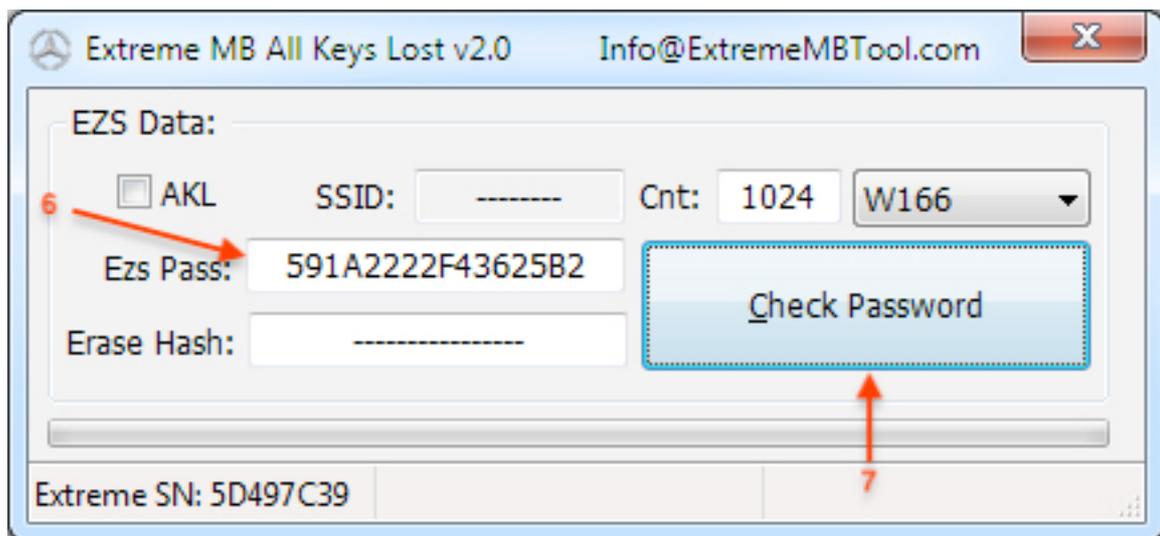
This is the field where we can enter the calculated Dealer Password if we want to "Renew the EZS". We can calculate this Dealer Password using the Extreme MB tool software. When the software detects that there is a Dealer Password entered into the "Erase Hash" field and it also detects that an EZS Password is present inside the "EZS Pass" field, then we will see that the text on the button becomes "ReNew EZS" This button can now be used to "Renew EZS"

## 7. Check Password Button

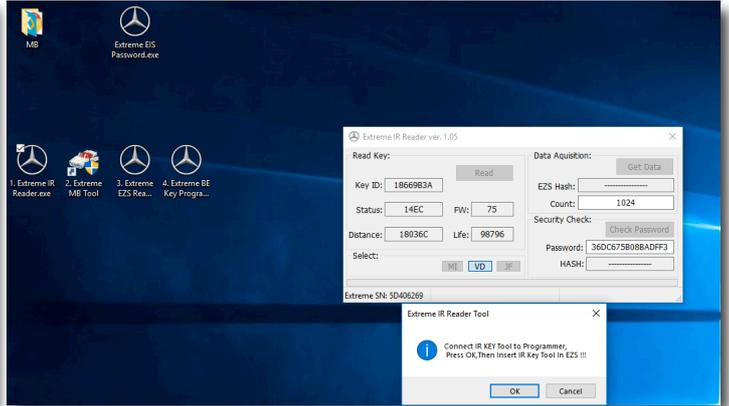
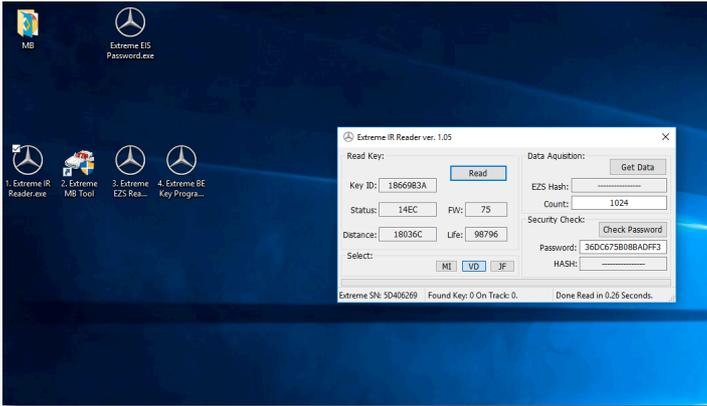
When a password is entered into the "EZS Pass" field, the text on the button becomes "Check Password". If you press the "Check Password" button the software will check if the password is a match with EZS.

## 9. ReNew EZS Button

You use this button to "ReNew the EZS"

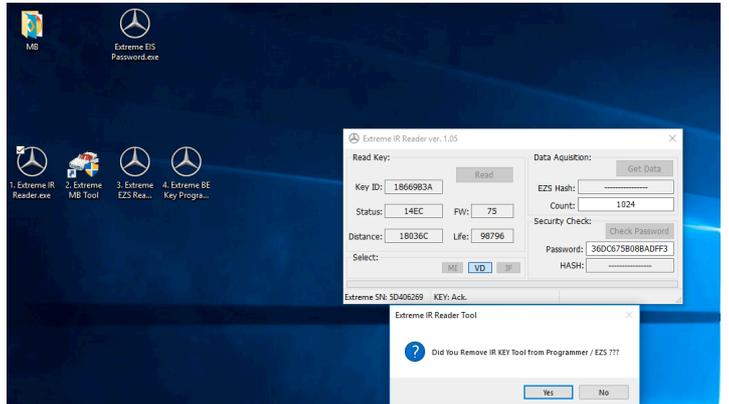
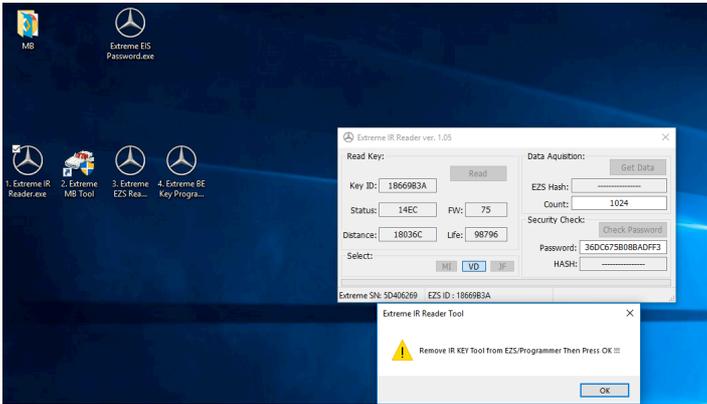


# Complete Key programming procedure when working key is available



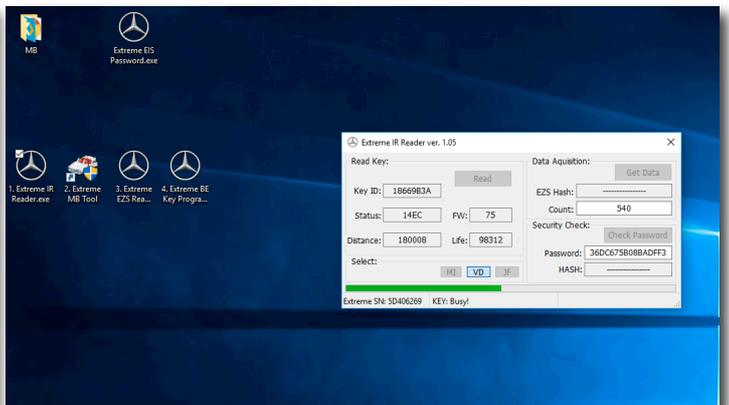
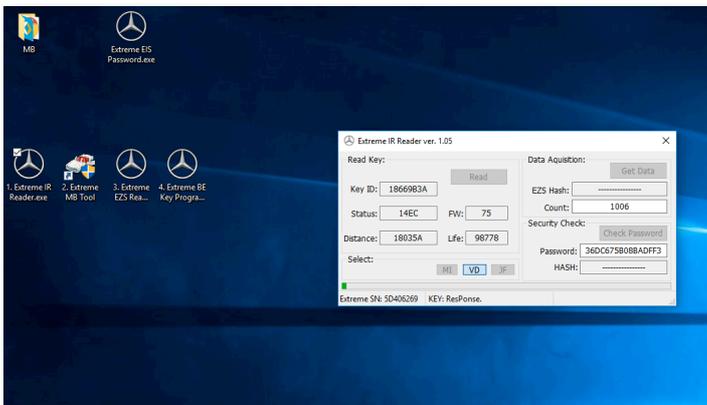
The first thing you will need to use is our software that reads data from the working key - "Extreme IR Reader". Open this software and press the "Read" button on user interface.

You must have IR Key Tool also connected to the IR Programmer. The software will ask you to insert IR Key Tool into the EZS, here we make a preliminary check to ensure the Key is a match with the EZS. If all is ok, we move onto reading the data from the working Key.



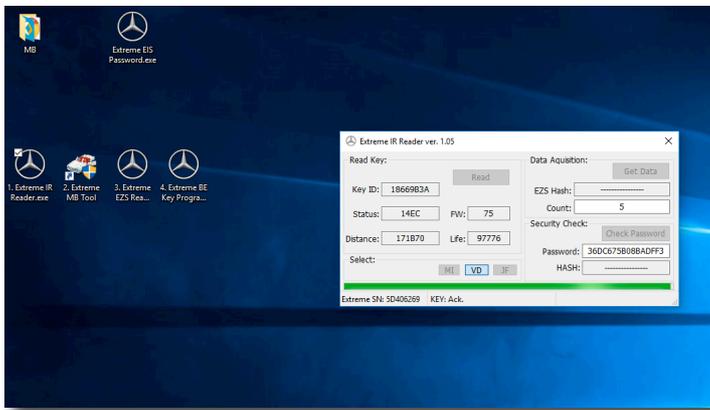
The procedure is very simple. Just follow the steps and execute exactly the explanations that software shows you

Just follow all steps

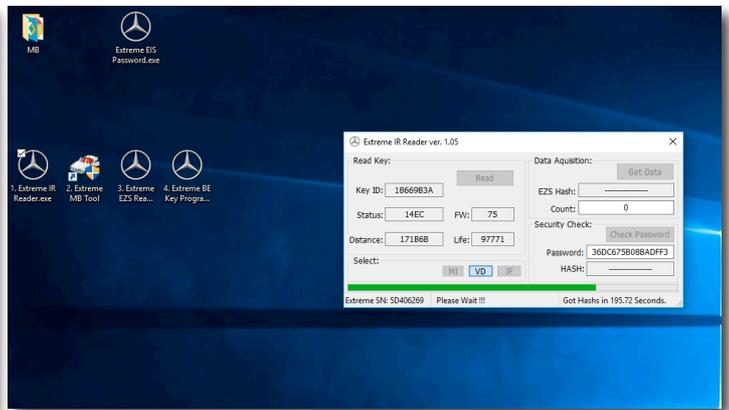


Above screenshot shows the process of reading data from the working key. You will notice the value displayed inside the "Count" field decrementing as we continue to read data from the working Key.

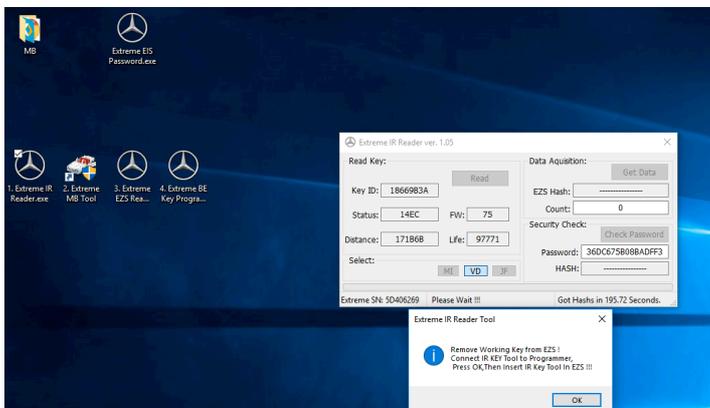
We recommend not to interfere with the IR Programmer Hardware or the Software while reading data from the working Key, please allow process to finish uninterrupted. When working with BGA Keys the Reading of the data from working key requires ~ 3 minutes. NEC keys can require ~ 8 minutes to get data.



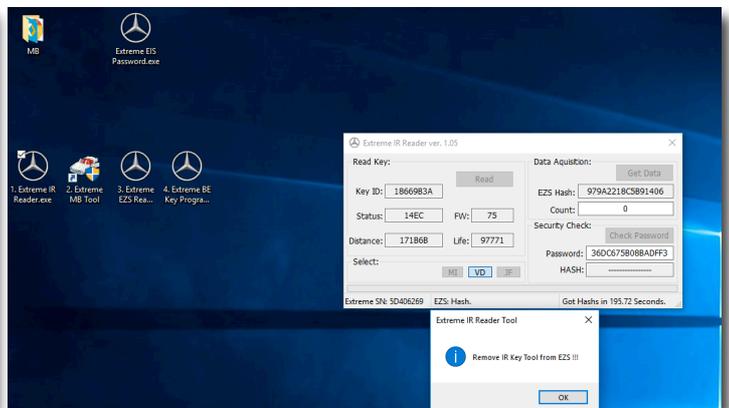
Final phase of reading the data



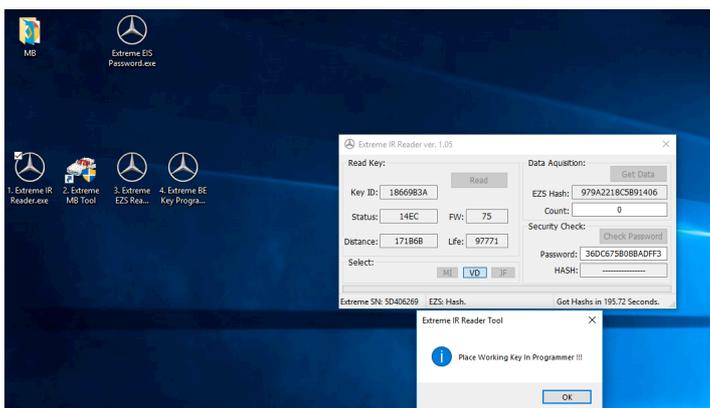
Remove the working key from the programmer and place it inside EZS for 30 seconds



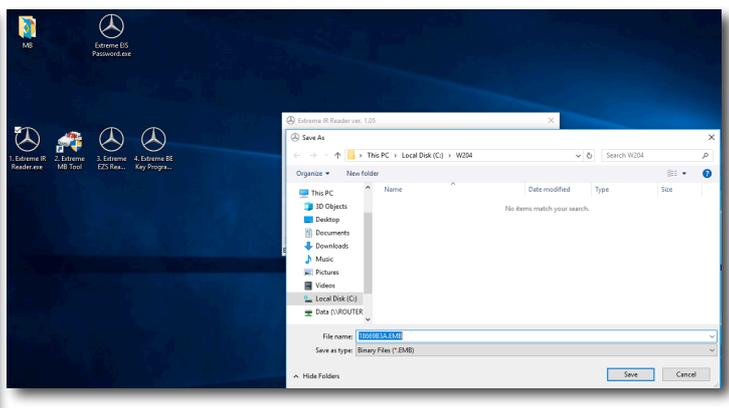
Follow the next step



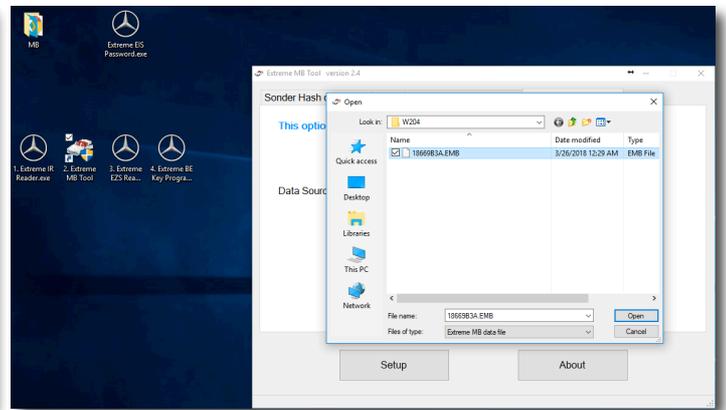
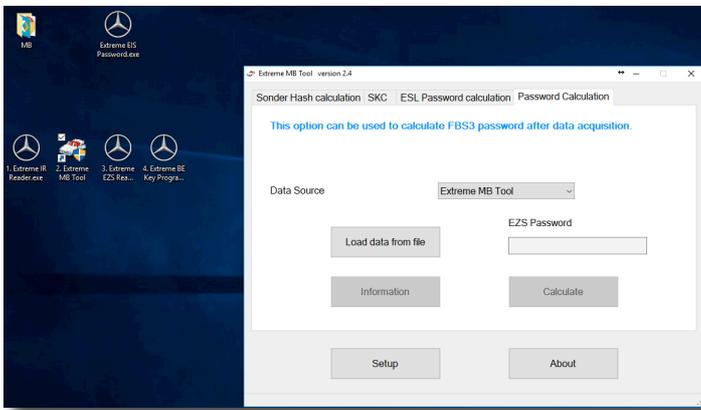
Follow the next step



Completing the data reading from working Key procedure

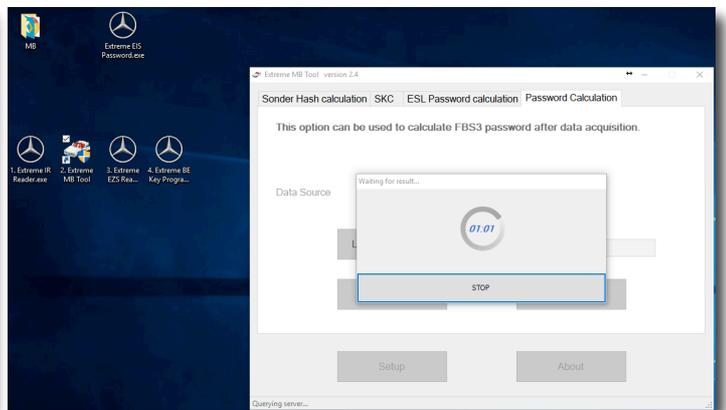
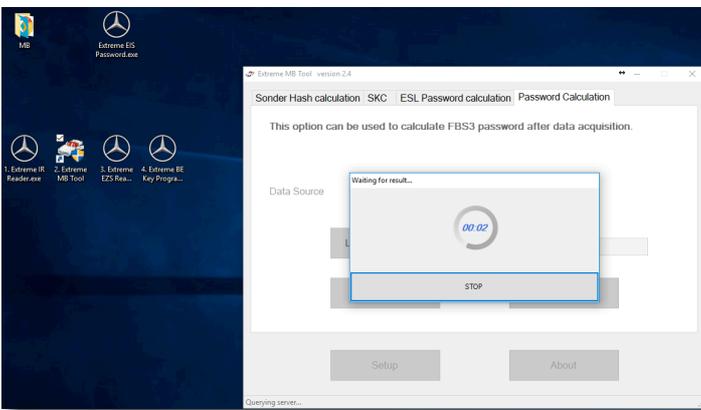


The Final step of reading the data from a working key will create a file containing the data needed to calculate the Keys Password. The default file name consists of the SSID of the Key and it will be saved with the extension .emb



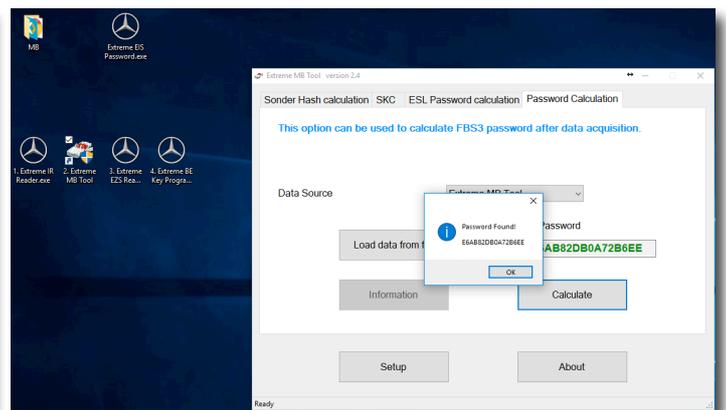
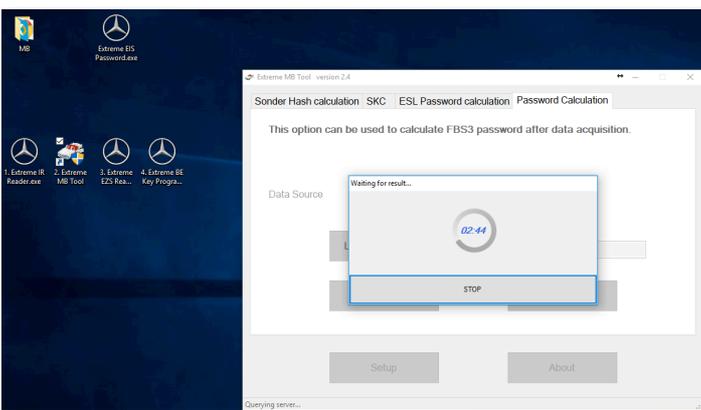
The next step is to search for the password from the created file. You have to use our "Extreme MB Tool" software. Choose from the Tab at the top of user interface – "Password Calculation" and from Data Source menu you need to choose "Extreme MB tool"

Load the file and press "Calculate"

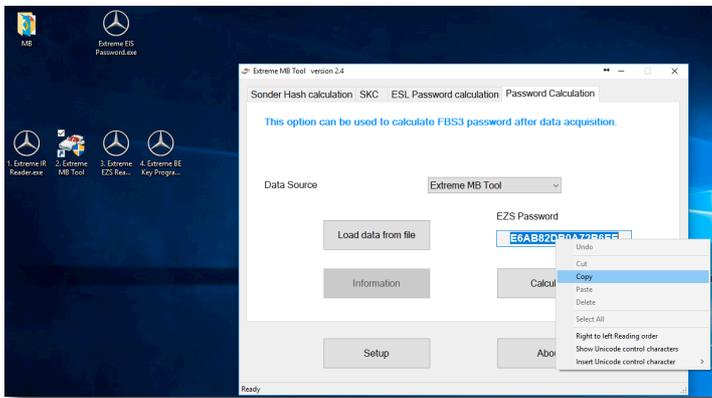


The password counting time is about 3 minutes

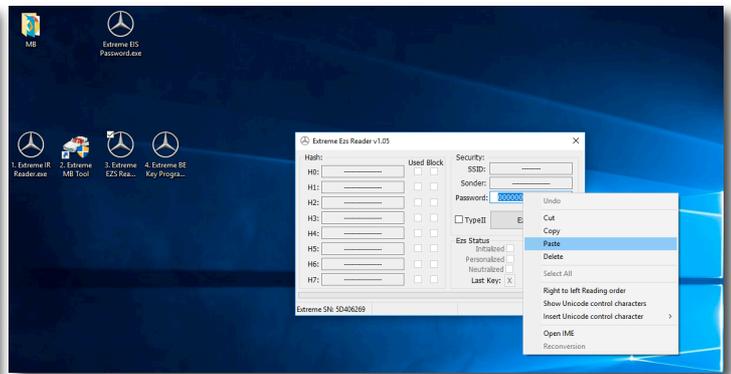
You must have an Internet connection



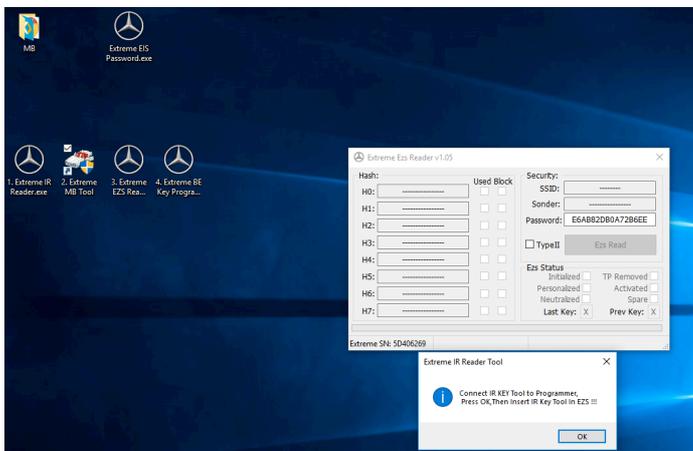
The password was calculated successfully



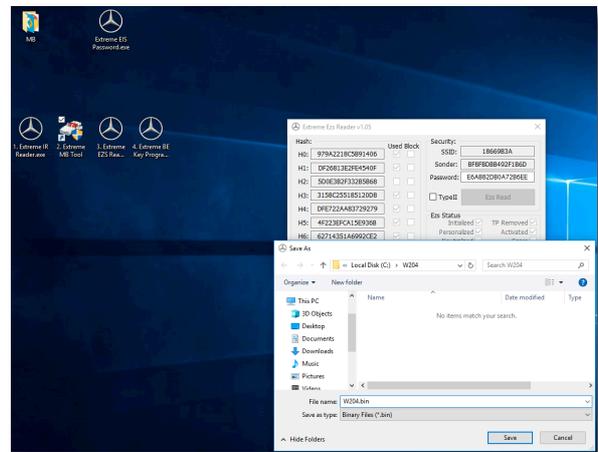
Copy the password to the clipboard



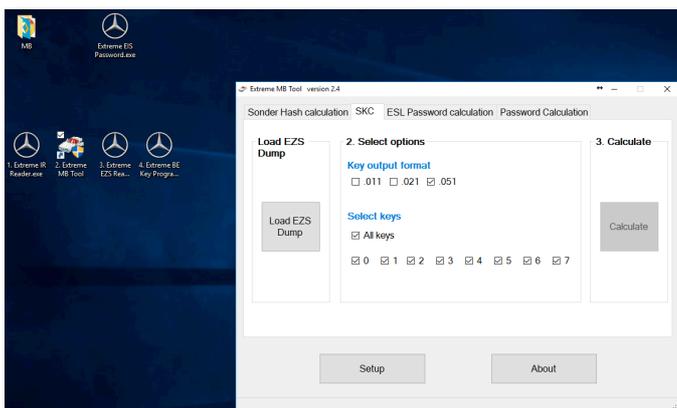
The next step is to read the EZS data via the infrared port on EZS. This will be done using our "Extreme EZS Reader" software. Before you start reading, you must paste the calculated Password from clipboard into the Password field of the Extreme EZS Reader user interface.



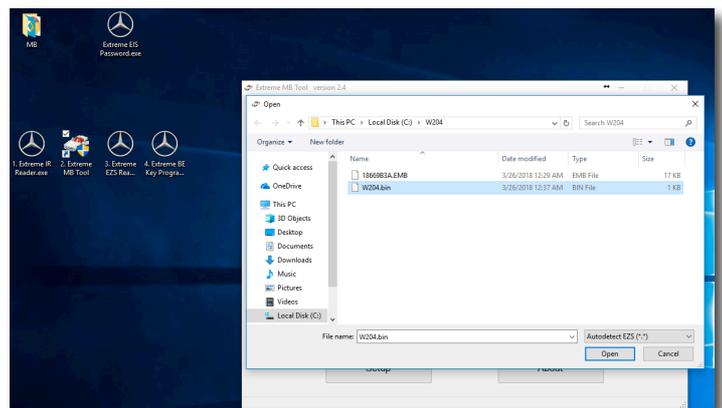
Press "EZS Read" button and follow the steps outlined in the software



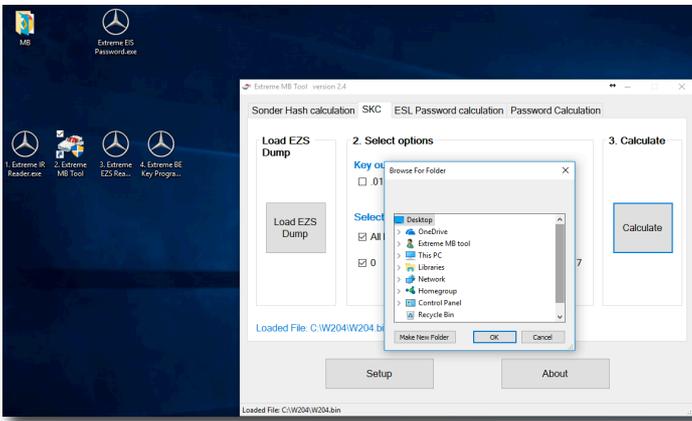
Extreme EZS Reader software will create a dump that is ready to be used with SKC to generate the key files. EZS file will be saved with the extension .ezs



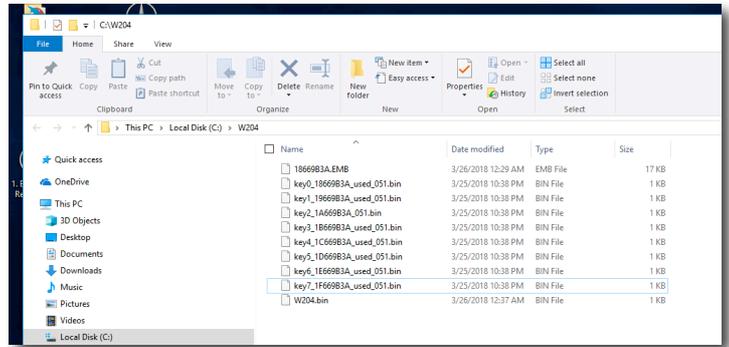
Open Extreme MB Tool software and select SKC from the Tab at the top of user interface. Then choose which keys you would like calculated, or by default the software will choose "All Keys" for you. Also by default we select the "Key Output Format" to be "051" We do this because this is the most popular format, and this is the format we use when working with BE Keys.



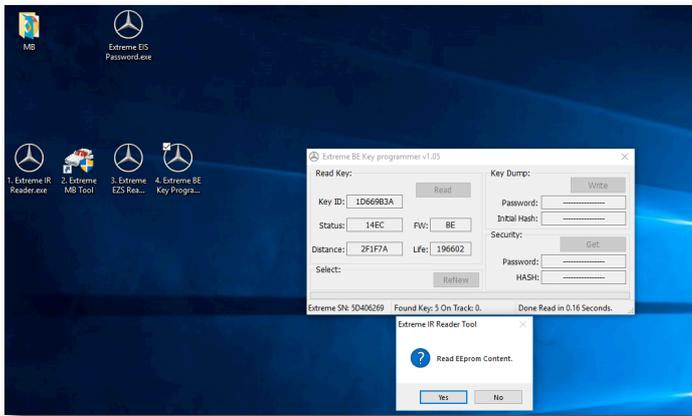
Now press the button "Load EZS Dump" and select the .ezs file that you read earlier from the EZS via the infrared port using our Extreme EZS Reader software.



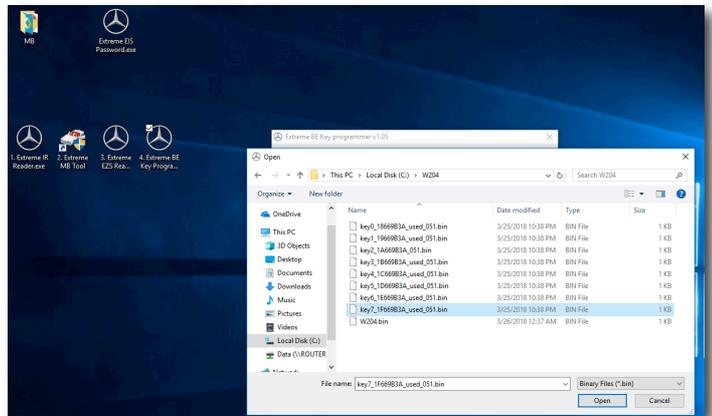
Select the folder where you want the keys files to be automatically saved



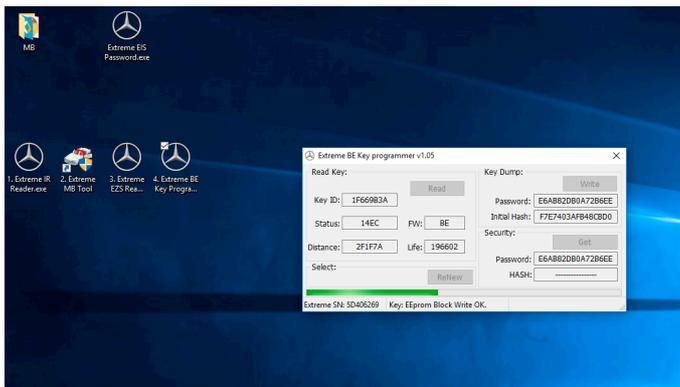
After a few seconds the key files are ready. Keys will also be labeled "Used" if the key position has already been used sometime previously



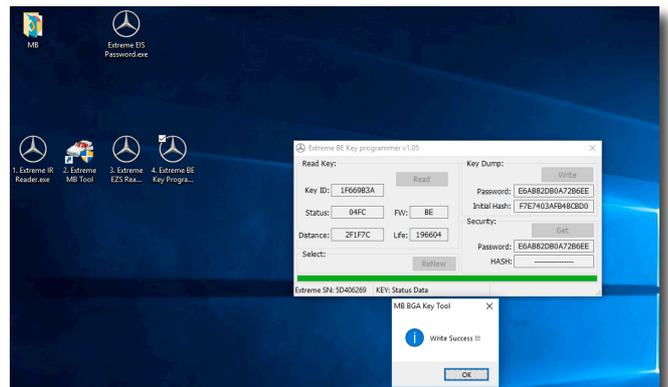
With "Extreme BE Key programmer" software you can very easily write any of the generated Key files to a BE Key via infrared. You can also make a "BE" key – renew (21DF Status)



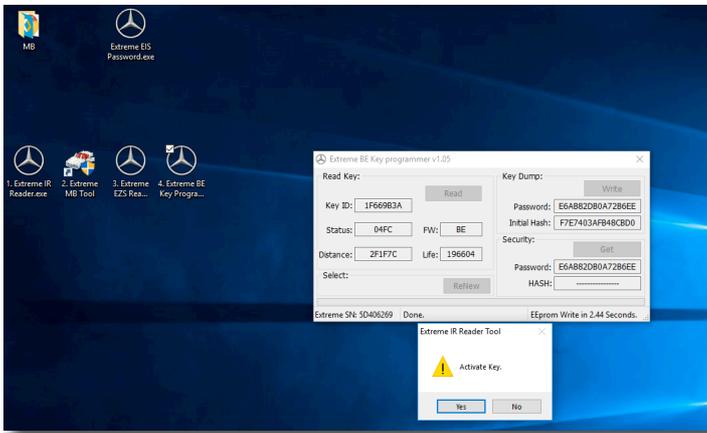
To write a Key file to a BE Key we need to press the "Write" Button on Extreme BE Key Programmer software. Then select the Key file that corresponds with the key position that you wish to use.



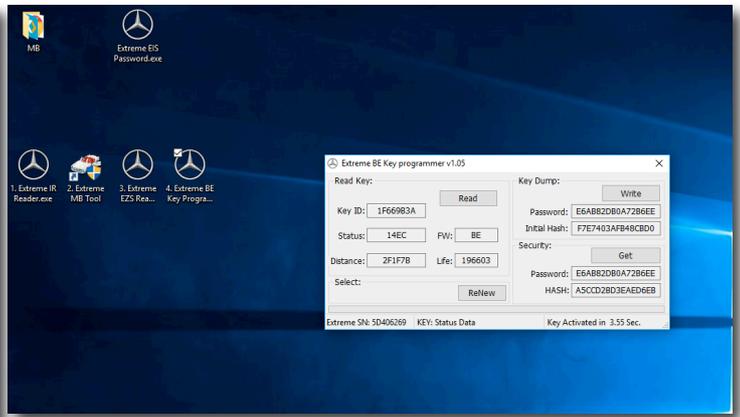
Writing Key file data into the BE key



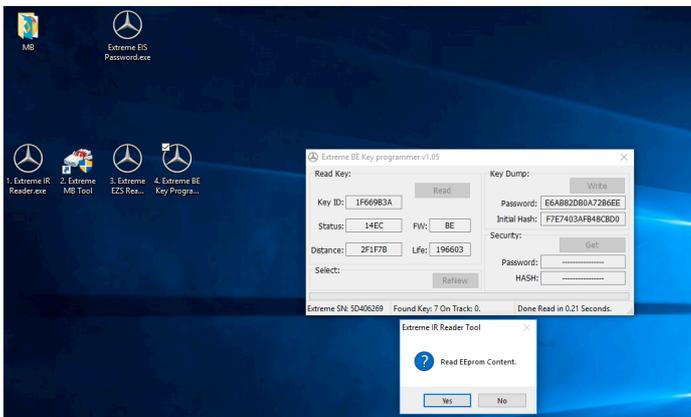
Successful writing of the Key file data into BE key



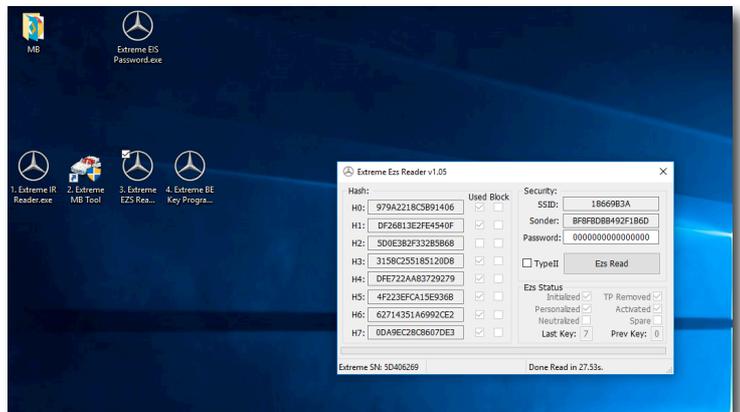
After successful data programming in the key, you have an option to activate the BE Key. This option is here because some older EZS such as HC705 types do not always activate BE keys after successful authentication. When working with these older EZS it is good practice to use this function within software to activate BE key after writing



If you decide to use the "Activate Key" function within Software then after successful Key activation you will see a message bottom right on User interface displaying "Key Activated"



If you wish to read the Key again after Programming it, just use the "Read" button and you will see all the info relating to the BE Key displayed, including the Keys SSID, it can be clearly seen here as the same SSID as the Key 7 file we programmed into it earlier. Also the Extreme BE Key Programmer Software gives you the option to read the full Key Dump from the BE Key. This can be seen on the screenshot above. It can be useful should you wish to verify that the key dump you have written to the BE Key is the same as the one you had intended to write.



After using the programmed Key 7 on the EZS you can read again the EZS with "Extreme EZS Reader" and you will see that the software will display Key Position 7 now as being a "Used" Position. And also, you will notice that now the software displays that Key 7 was the last key used on this EZS.

**NOTE:** When working with cars with 7G transmission, it can happen that 7G transmission requires a little extra time to sync with the other FBS3 components on the vehicle. You will know that this has happened if you can start the car ok, but the car will not select any gear. When this happens, all that is required is to start the car and allow it to idle for few minutes. This will allow the MCU inside the 7G control unit to "Catch up" with the other control units